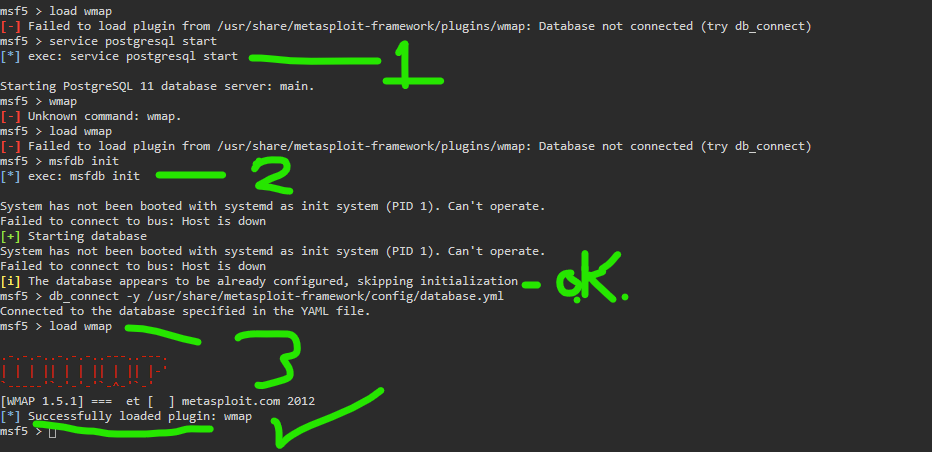
Wmap exploit

We know that there’s a web server… use wmap from within Metasploit as a plugin

If there’s no database connected, you’ll have to command: msfdb init

The load wmap

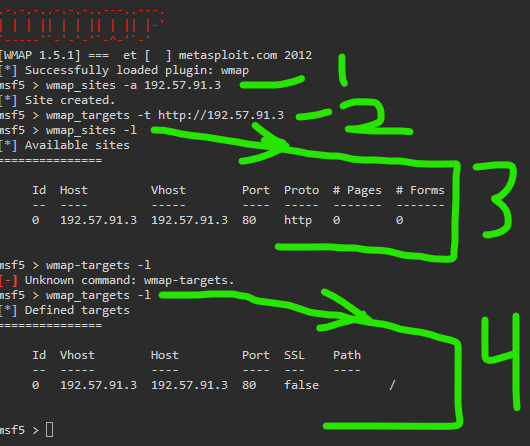


Command: wmap\_sites -a ip.add.re.ss

^Adds a site at an ip address

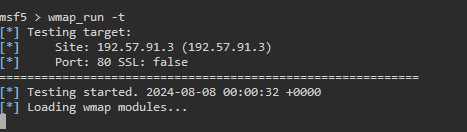
Wmap\_targets -t <http://ip.add.re.ss>

^ adds a target, which can then be seen by listing with -l for either

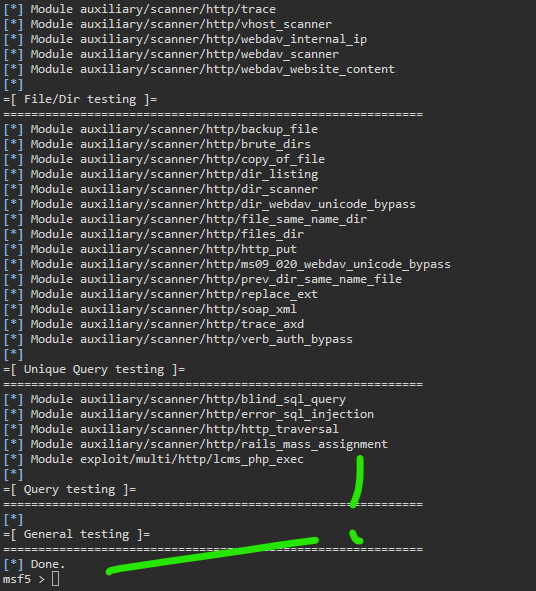


…

Actually execute the vulnerability scan with wmap\_run -t

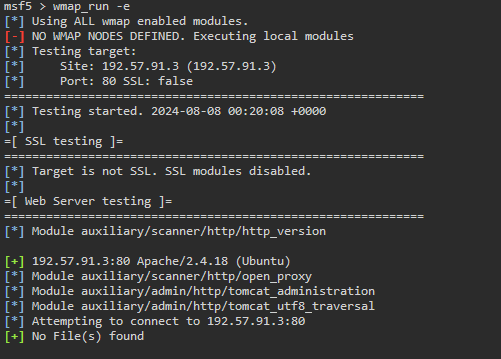


Shows results of wmap being done



Run all enabled exploit scripts against target

Command: wmap\_run -e



The following is the file enumeration, which was the goal of the lab. Yeah, the instructors were very vague about the purpose of this lab so it ends here…

